AMENDMENTS TO THE SPECIFICATION

Please replace paragraph [0005] with the paragraph below:

[0005] Today's firmware architectures include provisions for extending BIOS

functionality beyond that provided by the BIOS code stored in a platform's BIOS device (e.g.,

flash memory). More particularly, the Extensible Firmware Interface (EFI) (specifications and

examples of which may be found at http://developer.intel.com/technology/efi) is a public

industry specification that describes an abstract programmatic interface between platform

firmware and shrink-wrap operation systems or other custom application environments. The EFI

framework include provisions for extending BIOS functionality beyond that provided by the

BIOS code stored in a platform's BIOS device (e.g., flash memory). EFI enables firmware, in

the form of firmware modules and drivers, to be loaded from a variety of different resources,

including primary and secondary flash devices, option ROMs, various persistent storage devices

(e.g., hard disks, CD ROMs, etc.), and even over computer networks.

Please replace paragraph [0074] with the paragraph below:

[0074] In the foregoing embodiments, variables are first encrypted and then compressed.

This is merely an exemplary ordering, as variables could be first compressed and then encrypted.

In one embodiment, a symmetric encryption scheme, such as defined by the Advanced

Encryption Standard (AES) agency's federal information processing standard (FIPS) 197

(http:/csrc.nist.gov/publications/fips/fips197/fips-197.pdf).

Application No.: 10/561,049 Examiner: DAS Attorney Docket No.: 42P16112 -2-